パケットヘッダのパターン解析による未知の不正アクセスの検出

3H－02

松永 武　安井 浩之　松山 実

武蔵工業大学

1. はじめに

ネットワーク社会の急速な拡大に伴い，ネットワークを利用した不正行為・犯罪による被害が世界的に深刻化しつつあり，セキュリティ対策として，FireWall によるアクセス制限，SSL 等の暗号化，侵入検知システム(IDS：Intrusion Detection System)の導入などが行われている．特に不正アクセスに関しては FireWall と IDS を組み合わせた構成が望ましいといわれている．[1]

IDS の不正アクセスを検出する方法には，不正検出と異常検出がある．不正検出はあらかじめ不正アクセスの情報をシグネチャに登録しておき，入力イベントと比較することで不正アクセスを検出する．一方，異常検出は正常時における入力イベントから正常時のプロファイルを作成しておき．入力イベントとプロファイルを比較して，差異が大きいとき異常とする．この方法は未知の不正アクセスを検出することが期待できるが，プロファイル作成に関する決定的な手法は確立しておらず，実用的なシステムにおいては不正検出が用いられている．[2]

本稿では，パケットヘッダの時系列データをパターン解析した結果をプロファイルとするホストベース型の IDS を提案する．

2. システム構成

システムの構成図を Fig.1 に示す．本システムでは各クライアントでパケットヘッダの特徴を検出し，異常が発生した場合に監視サーバに情報を送ることで，ネットワーク全体に対する攻撃に対処できる．利点として，ネットワークベース型 IDS[2]よりも負荷が軽減できることがあげられる．また，各クライアントのシステムイベント(メモリの変化，アプリケーションログなど)の情報も取得できる．ただし，各クライアントで異常検出を行うのでクライアントに負荷がかかること，監視サーバに情報を送ることで，ネットワークに負荷がかかることなどの欠点も考えられる．

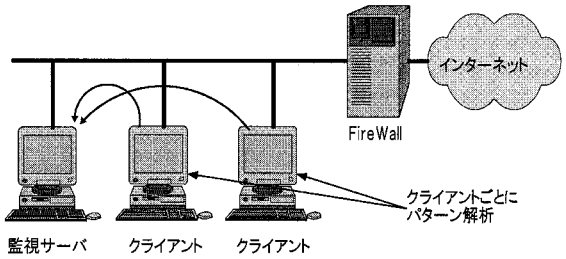

Fig.1　構成図

3. パターン解析

本稿では，クライアントで受信したパケットヘッダのパケット長を調べ，正常時との誤差を求めることで検出する方法について検証した．しかし，そのままパケット長を取得しても，特長がみられないので，ポートごとで分割する方法を方法について検証した．

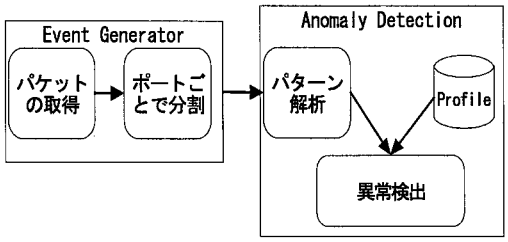

Fig.2 ポートごとで分割

The anomaly detection with pattern analysis of packet header
Takeshi Matunaga, Hiroyuki Yasui ,Minoru Matuyama
Musashi Institute of Technology

3.1 時系列におけるパケット長の相関関係

プロファイルするためには，正常時のデータの特徴を調べておく必要がある．Fig.3,4 は時系列でのパケット長の相関関係を示した図である．この図はセッション開始から終了までのパケット長の時系列データを *x(t)* とし，

$x=x(t)$　　$y=x(t+1)$

の関係をプロットしたものである．Fig.3 は送信元ポート番号が SSH で分割した時系列データであり，プロットしたパケットの総数は 1000 である．同様に，Fig.4 は HTTP であり，パケットの総数は 3000 である．

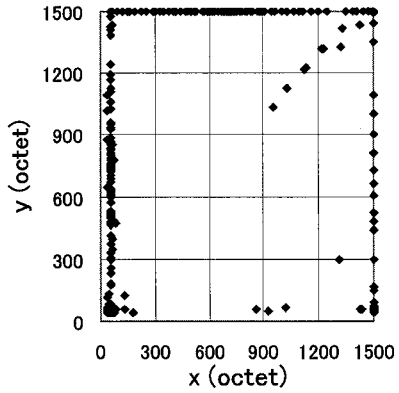

Fig.3　*x(t)* と *x(t+1)* の関係(SSH)

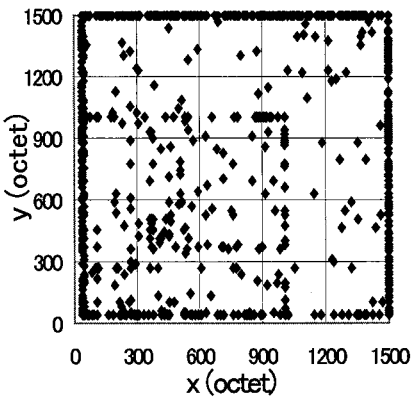

Fig.4 *x(t)* と *x(t+1)* の関係(HTTP)

ポートごとでパケット長の *x(t)* と *x(t+1)* の関係を調べると，SSH はマップの端に偏り，HTTP も同様マップの端に偏るが，中は分散した形になり，ポートごとの特徴が出ていることがわかる．よって *x(t)* と *x(t+1)* の関係をプロファイルとして作成できることになる．

3.2 検出方法

3.1 で作成した相関関係をプロファイルとし，入力されたパケットデータとの比較を行う方法は現在考察中だが，*x(t)* と *x(t+1)* が重なり合う数を度数分布で表現したものをプロファイルにすることを考えている．

4. まとめ

本稿では時系列データの *x(t)* と *x(t+1)* の関係による有用性について述べた．今後の課題として，プロファイルした *x(t)* と *x(t+1)* の関係を異常な時系列のデータを判断する方法の決定，本稿ではパケット長だけについて述べたが，他のパラメータ(他のパケットヘッダやシステムイベントなど)での測定を行い，有効なパラメータを特定することが必要である．

参考文献

[1]IPA ISEC（セキュリティセンター）
http://www.ipa.go.jp/security/

[2]武田圭史　侵入検知システムに関する研究の現状　情報処理 Vol.42 No.12 情報処理学会 pp.1169-1174